БЕЗОПАСНОСТЬ ТЕХНОЛОГИИ RFID

[1]**Ибрагимов В.Р., Папуловская Н.В.**

[1]*ФГАОУ ВПО УрФУ, ИРИТ-РТФ, г. Екатеринбург*

В данной статье описывается технология RFID, и рассматривается проблема безопасности при её использовании в платёжных системах, системах контроля доступа, и других системах безопасности.

Ключевые слова: Технология RFID, беспроводные карты, RFID- метки, безопасность.

Введение:

Технология RFID (англ. Radio Frequency Identification, радиочастотная идентификация) – способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. Любая RFID-система состоит из считывающего устройства и транспондера (иногда также применяется термин RFID-тег) [1]. Работает эта система посредством электромагнитных волн определённой частоты. Так же данная технология используется в данное время в магазинах, супермаркетах, торговых центрах для защиты товаров от краж. [2]. Система беспроводной авторизации в помещения ограниченного доступа используются на проходных, на закрытых объектах, и для идентификации объектов, в том числе и людей [3].

В настоящее время эта технология широко используется во многих областях нашей деятельности, например: маячки в магазинах, беспроводные карты доступа на проходных, на парковки, платёжные карты, дисконтные карты и многое другое.

Цель исследования:

Несмотря на то что эта технология так широко используется в повседневной жизни, безопасность её оставляет желать лучшего. Практически к любой карте RFID можно получить доступ без ведома её владельца. И по этой причине актуальна проблема безопасности в этой технологии.

Материал и методы исследования:

Сейчас в свободной продаже доступны различные считывающие и записывающие устройства. Различные RFID-метки работают на различных частотах:

- Метки диапазона LF (125—134 кГц)
- Метки диапазона UHF (860—960 МГц)
- Радиочастотные UHF- метки ближнего поля

Соответственно под каждый вид меток существуют различные считыватели и записывающие устройства. Большинство меток можно только прочитать. Запись осуществляется только на специальные метки, их производство обходится немного дороже.

Метки бывают активными и пассивными. Активные метки при определённом уровне излучения от считывателя начинают отправлять сигнал, в своём составе они имеют элемент питания, либо работают от какой-либо электросети. Пассивные метки используют энергию излучения считывателя. Соответственно пассивные метки дешевле в изготовлении и прочнее в практическом применении, не требует дополнительных затрат при использовании, но у активных меток больше радиус действия.

Для исследования были приобретены считыватели, работающие на частоте 125 кГц и 13,6 МГц.

В качестве примера рассмотрим протокол EM4100 работающий на частоте 125 кГц. В пассивной метке как только напряжение возрастает до уровня срабатывания, метка отправляет 64-битный двоичный код. В начале кода передаются девять еденицы, обозначающие шачало данных, затем передаётся код, который разбивается по пять бит, первые четыре бита переводятся в шестнадцатиричное число, пятый- это контрольная сумма предыдущих четырех. Так следуют десять «пятёрок», затем передаётся побитовая контрольная сумма всех шестнадцатиричных чисел. После следует нулевой стоп-бит. Покажем на конкретном примере:

111111111 00101 11000 00000 00000 01111 01111 01010 01010 10100 00101 0110 0

Таблица 1.Пример разбиения передаваемого кода

Код	Шестнадцатиричное значение	Контрольная сумма
00101	2	1
11000	C	0
00000	0	0
00000	0	0
01111	7	1
01111	7	1
01010	5	0
01010	5	0
10100	A	0
00101	2	1
0110 – Побитовая сумма		

Для несанкционированного доступа к закрытым дынным достаточно знать первоначальный двоичный код. Далее злоумышленник может записать этот код на карту и пользоваться доступом к определённым ресурсам.

Достаточно повысить безопасность помогут банальные меры предосторожности, например кнопка, замыкающая колебательный контур антенны, или ввод пароля после считывания идентификационного номера, как на банковских картах. Конечно на сто процентов защитить карту от взлома вряд ли получится, но существенно повысить её можно.

Выводы и заключение:

Рассматриваемая технология нуждается в доработке, потому как в настоящее время используется во многих сферах нашей деятельности и не сильно безопасна в плане конфиденциальности данных, хранящихся на чипе. Но для обыкновенной идентификации эта технология подходит очень хорошо и используется совсем немного, например, это достойная замена штрих-кодам, беспроводную метку легко обезопасить от механического воздействия. Плюс к этому можно хранить намного больше данных в метке и, следовательно, можно пронумеровать гораздо больше товаров или различных вещей, нуждающихся в индивидуальном учете, на метки диапазона UHF можно даже записать немного информации о товаре.

Доработав эту технологию можно сильно облегчить повседневную жизнь, а также обезопасить данные, хранящиеся на беспроводном носителе.

Список литературы:

1. https://ru.wikipedia.org/wiki/RFID
2. http://habrahabr.ru/post/161401/
3. http://habrahabr.ru/post/182846/